# PROTEKSI INTEGRITAS DATA DENGAN METODE CRC32 DAN SHA-256 PADA APLIKASI PENGUNDUH DAN TRANSFER FILE

Oleh

Bagus Pradipta Satriyajati Hutomo

NIM: 622013007

Skripsi

Untuk melengkapi salah satu syarat memperoleh

Gelar Sarjana Teknik

Program Studi Sistem Komputer

Fakultas Teknik Elektronika dan Komputer

Universitas Kristen Satya Wacana Salatiga

Desember 2017

# PROTEKSI INTEGRITAS DATA DENGAN METODE CRC32 DAN SHA-256 PADA APLIKASI PENGUNDUH DAN TRANSFER FILE

Oleh
Bagus Pradipta Satriyajati Hutomo
NIM: 622013007

Skripsi ini telah diterima dan disahkan
Untuk melengkapi salah satu syarat memperoleh
Gelar Sarjana Teknik
dalam
Konsentrasi Jaringan Komputer dan Telekomunikasi
Program Studi Sistem Komputer
Fakultas Teknik Elektronika Dan Komputer
Universitas Kristen Satya Wacana
Salatiga

Disahkan oleh

| Pembimbing I | Pembimbing II |
| --- | --- |
| Hartanto Kusuma Wardana, M.T. | Banu Wirawan Yohanes, M.CompSc. |
| Tgl. 31/1/18 | Tgl. 1-2-2018 |

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

# PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan di bawah ini:

Nama : Bagus Pradipta Satriyajati Hutomo

NIM : 672013007 Email : 672013007@student.uksw.edu

Fakultas : FTEK Program Studi : Sistem Komputer

Judul tugas akhir : Proteksi Integritas Data dengan Metode CRC32 dan SHA-256 pada Aplikasi Pengunduh dan Transfer File

Pembimbing : 1. Hartanto Kusuma Wardana, M.T.

2. Banu Wirawan Yohanes, M.Compsc.

Dengan ini menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar kesarjanaan baik di Universitas Kristen Satya Wacana maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian/implementasi saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing akademik dan narasumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan disetujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Kristen Satya Wacana.

Salatiga, 31 Januari 2018


Bagus Pradipta Satriyajati H.

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

# PERNYATAAN PERSETUJUAN AKSES

Saya yang bertanda tangan di bawah ini:

Nama : Bagus Pradipta Satriyajati Hutomo
NIM : 672013007 Email : 672013007@student.uksw.edu
Fakultas : FTEK Program Studi : Sistem Komputer
Judul tugas akhir : Proteksi Integritas Data dengan Metode CRC32 dan SHA-256 pada Aplikasi Pengunduh dan Transfer File

Dengan ini saya menyerahkan hak *non-eksklusif** kepada Perpustakaan Universitas – Universitas Kristen Satya Wacana untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tugas akhir elektronik sebagai berikut (beri tanda pada kotak yang sesuai):

☑ a. Saya mengijinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA

☐ b. Saya tidak mengijinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA**

* *Hak yang tidak terbatas hanya bagi satu pihak saja. Pengajar, peneliti, dan mahasiswa yang menyerahkan hak non-eksklusif kepada Repositori Perpustakaan Universitas saat mengumpulkan hasil karya mereka masih memiliki hak copyright atas karya tersebut.*

** *Hanya akan menampilkan halaman judul dan abstrak. Pilihan ini harus dilampiri dengan penjelasan/ alasan tertulis dari pembimbing TA dan diketahui oleh pimpinan fakultas (dekan/kaprodi).*

Demikian pernyataan ini saya buat dengan sebenarnya.

Salatiga, 31 Januari 2019

Bagus Pradipta Satriyajati H.
*Tanda tangan & nama terang mahasiswa*

Mengetahui,

Hartanto Kusuma Wardana, M.T.
*Tanda tangan & nama terang pembimbing I*

Bayu Wirawan Yohanes, M.Comp.Sc.
*Tanda tangan & nama terang pembimbing II*

# INTISARI

Seiring file yang tersebar luas di internet, dibutuhkan perangkat lunak untuk mengecek integritas dan keamanan data setelah file diunduh atau ditransfer. Selain unduh dan transfer cek integritas juga dilakukan saat pengiriman file penting seperti dokumen. Untuk melakukan cek integritas dan keamanan data, digunakan nilai CRC32 dan SHA-256. Metode yang digunakan adalah dengan membangkitkan nilai CRC dan SHA saat pembuatan file khusus sebelum file diunggah. File yang diunduh atau transfer dicek dengan cara membandingkan nilai CRC dan SHA yang terdapat pada file, dan nilai CRC dan SHA yang dihitung oleh perangkat lunak. CRC32 dan SHA-256 dapat mendeteksi perubahan 1 bit pada file, sehingga CRC32 dan SHA-256 mampu untuk memeriksa integritas dan keamanan data.

| Mengetahui, | Mengesahkan, | Penyusun, |
|---|---|---|
| Hartanto K. Wardana, M.T. | Hartanto K. Wardana, M.T. | Bagus Pradipta S.H. |
| Dekan | Pembimbing | |

## ABSTRACT

As files are widespread on the internet, software is required to check the integrity and security of data after the files are downloaded or transferred. In addition to download and transfer integrity checks are also done when sending important files such as documents. To perform these checks, CRC32 and SHA-256 values were used. The method is to generate CRC and SHA values when creating a special file before the files were uploaded. Downloaded or transferred files were checked by comparing the CRC and SHA values which these are contained in the file and the CRC and SHA values which were calculated by the software. CRC32 and SHA-256 can detect 1 bit changes in files, so CRC32 and SHA-256 are able to check data integrity and security.

## KATA PENGANTAR

Puji Syukur kepada Allah Bapa karena atas berkat yang melimpah, skripsi ini mampu diselesaikan. Dimulai tahun 2013 saat memulai awal kuliah hingga membuat skripsi ini, banyak pengalaman yang sudah dijadikan pelajaran, semua karena penyertaan Yesus Kristus Putramu.

Terima kasih pula kepada semua yang sudah mendukung secara langsung maupun tidak langsung dalam penulisan skripsi ini. Penulis mengucapkan terima kasih kepada:

1. Hartanto Kusuma Wardana, M.T., sebagai Dekan Fakultas Teknik Elektro dan Komputer dan pembimbing I.
2. Banu Wirawan Yohanes, M.ComSc., sebagai pembimbing II.
3. Seluruh Dosen dan Staf Fakultas Teknik Elektro dan Komputer.
4. Kedua orang tua yang saya cintai, yang sudah mendukung hingga kini. Juga kepada keluarga semuanya.
5. Teman-teman angkatan 2013, khususnya penghuni *channel* Discord yang sudah menggarami dan rela digarami.

**DAFTAR ISI**

## DAFTAR GAMBAR

## DAFTAR TABEL

## DAFTAR LAMBANG

| | |
|---|---|
| *Ch* (*x,y,z)* | *choose* pada fungsi SHA-256 |
| *Maj* (*x,y,z*) | *Major* pada fungsi SHA-256 |
| $\sum_0 (x)$ | Sigma 0 pada fungsi SHA-256 |
| $\sum_1 (x)$ | Sigma 1 pada fungsi SHA-256 |
| $\sigma_0 (x)$ | sigma 0 pada fungsi SHA-256 |
| $\sigma_1 (x)$ | sigma 1 pada fungsi SHA-256 |
| *x, y, z* | Variabel pada fungsi SHA-256 |
| *W* | Pesan pada SHA-256 |
| N | Jumlah pesan pada SHA-256 |
| $\wedge$ | Operasi AND |
| $\oplus$ | Operasi XOR |
| $\neg$ | Operasi Not |
| *ROTR* $^n$ | *Rotate right* sebanyak *n*-bit ((x >> n) \| (x << w - n)) |
| *SHR* $^n$ | *Shift right* sebanyak *n*-bit (x >> n) |
| + | *Additon modulo* $2^{32}$, jika hasil penambahan melebihi 32-bit di-*modulo* $2^{32}$ |
| *K* | Konstan |
| *l* | Panjang pesan untuk 1 blok pesan |
| *k* | Jumlah *padding* 0 bit |
| *H* | Nilai *hash* |

## DAFTAR SINGKATAN

| | |
|---|---|
| LAN | *Local Area Network* |
| CRC | *Cyclic Redundancy Check* |
| SHA | *Secure Hash Algorithm* |
| HTTP | *Hpertext Transfer Protocol* |
| HTTPS | *Hpertext Transfer Protocol Secure* |
| WWW | *World Wide Web* |
| TCP | *Transport Control Protocol* |
| FTP | *File Transfer Protocol* |
| SMB | *Server Message Block* |
| NetBIOS | *Network Basic Input/Output System* |
| URL | *Uniform Resource Locator* |